

# **SUBMISSION TO ICO CALL FOR EVIDENCE ON AGE APPROPRIATE DESIGN CODE**

**UNICEF UK**

**19/09/2018**

## **SECTION ONE: VIEWS AND EVIDENCE**

UNICEF, the United Nations Children's Fund, is mandated by the UN General Assembly to uphold the Convention on the Rights of the Child and promote the rights and wellbeing of every child. Together with partners, UNICEF works in over 190 countries and territories to translate its commitment to the rights and wellbeing of every child into practical action, focusing special effort on reaching the most vulnerable and excluded children, to the benefit of all children, everywhere. Unicef UK (UUK) is one of 36 National Committees.

It is with this mandate that UUK submits evidence to the Information Commissioners Office on Age Appropriate Design. Its submission focuses on setting out how relevant rights frameworks, including the UNCRC as well as the UN Guiding Principles for Business and Human Rights should be applied in the context of upholding children's rights online. Within this, it highlights the need for the Code to reflect both the evolving capacities of children, as well as consider how specific vulnerabilities and risks faced by groups of children will affect the level of protection they require to uphold their rights. It sets out how underlying principles of best interests of the child and their right to be heard in should be taken into account when designing the Code, and then provides recommendations for each aspect of the Code from a rights-based perspective.

The submission makes the case for embedding transparency into the Code to ensure that commercial interests are not prioritised over those of the child, whereby decisions taken by businesses regarding the design of their services used by children are open to public scrutiny. It also recommends that the Code has pre-established moments for review, to ensure changes in the digital context can be reflected in the Code and any weaknesses in enforcement and application addressed.

## **DEVELOPMENT NEEDS OF CHILDREN AT DIFFERENT AGES**

### **QUESTION 1A**

1. In designing products and services for children, age is a useful consideration insofar as it offers a proxy for ability. Design standards should however be led by children's capacities, and while age brackets can give a useful idea of what standards might be appropriate, they should not set rigid

boundaries. In line with Article Three of the Convention on the Rights of the Child, the Code should provide flexibility to consider the evolving capacities of every child.<sup>1</sup>

2. However, whilst research on children's evolving capacities exists,<sup>2</sup> there is a lack of evidence about how these capacities translate into an online environment, and what specific capacities are required to navigate effectively and safely online. The risks that children face in the digital environment are dynamic, creating additional challenges for using age brackets to determine protective design features. For instance, advances in technology, which are increasingly embedded into home life are resulting in children becoming more connected in more ways from an ever younger age. A child's digital literacy is also not necessarily a linear progression; rather, children may encounter increasingly complex and challenging situations online as their skills and appetite to engage grow, the devices they use change, and adult oversight lessens. For instance, recent research by Global Kids Online in Bulgaria included targeted recommendations for 12-14 year olds due findings that at that age children start exploring and experimenting more with the internet while parental mediation and supervision decreases.<sup>3</sup>

3. Specific vulnerabilities of some children will also have a bearing on risks they face, for instance children who live independently under the age of 18, disabled children or those living with multiple health problems, children who have been victims of sexual exploitation and children in care may require additional or different types of protection. The Commission should consider referring to the Convention of the Rights of Persons with Disabilities in addition to the Convention of the Rights of the Child as a source of relevant international rights law. In light of these variables, age or capacity alone cannot determine the level of protection afforded to children, and the Code should consider the varying risks that children of different ages, capacities and vulnerabilities face in the digital environment.

## **CONVENTION ON THE RIGHTS OF THE CHILD**

### **QUESTION 3**

#### **Children's Rights & Business**

---

<sup>1</sup> Convention on the Rights of the Child, Article 3.

<sup>2</sup> See for instance, Gerison Lansdown, The Evolving Capacities of the Child, Save the Children & UNICEF (2005), available at <https://www.unicef-irc.org/publications/pdf/evolving-eng.pdf>

<sup>3</sup> See, e.g., Kanchev et al., Are Digital Natives Digitally Literate? Insights from a Representative Survey in Bulgaria (2016), available at <https://www.safenet.bg/images/sampled/data/files/Digital-and-Media-Literacy.pdf>

4. As the Code will regulate the activities of Information Society Services, which are largely offered by business entities, it should be firmly grounded in international standards that regulate business conduct, as outlined below. The Code should build on the established corporate responsibility to respect human rights, including children's rights as enshrined in the Convention on the Rights of the Child.

### **Corporate Responsibility to Respect Human Rights**

5. While governments have the primary obligation under international law to protect human rights, the United Nations has adopted Guiding Principles on Business and Human Rights that assert a corporate responsibility to respect human rights.<sup>4</sup> The Guiding Principles make clear that businesses are expected to conduct human rights due diligence, a process that involves “assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed.”<sup>5</sup> This means that companies have a responsibility to consider and address their impacts on human rights, including children's rights to privacy and freedom of expression.

6. The Government of the United Kingdom was the first in the world to publish a National Action Plan on Business and Human Rights, a policy document that sets out how the Government intends to implement the Guiding Principles. The Government published an updated National Action plan in 2016, which reaffirms the Government's commitment to the Guiding Principles and an expectation that UK companies “adopt appropriate due diligence policies to identify, prevent and mitigate human rights risks, and commit to monitoring and evaluating implementation.”<sup>6</sup> The ICO's approach to developing the Code is in line with the National Action Plan, and should seek to advance these commitments.

### **Corporate Responsibility to Respect Children's Rights**

7. The Guiding Principles should be “implemented in a non-discriminatory manner, with particular attention to the rights and needs of, as well as the challenges faced by, individuals from groups or

---

<sup>4</sup> Guiding Principles for Business and Human Rights: Implementing the United Nations 'Protect Respect and Remedy' Framework, Office of the United Nations High Commissioner for Human Rights (2011), available at [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf)

<sup>5</sup> United Nations Guiding Principles for Business and Human Rights, Principle 17.

<sup>6</sup> Good Business: Implementing the UN Guiding Principles on Business and Human Rights (May 2016), para. 21, available at [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/522805/Good\\_Business\\_Implementing\\_the\\_UN\\_Guiding\\_Principles\\_on\\_Business\\_and\\_Human\\_Rights\\_updated\\_May\\_2016.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/522805/Good_Business_Implementing_the_UN_Guiding_Principles_on_Business_and_Human_Rights_updated_May_2016.pdf)

populations that may be at heightened risk of becoming vulnerable or marginalized, and with due regard to the different risks that may be faced by women and men.”<sup>7</sup> The UN Secretary General’s Special Representative for Business and Human Rights responsible for developing the Guiding Principles has recognised that “[c]hildren are among the most marginalized and vulnerable members of society, and can be disproportionately, severely and permanently impacted by business activities, operations and relationships.”<sup>8</sup>

8. The Children’s Rights and Business Principles, developed by UNICEF, Save the Children and the UN Global Compact, call on all businesses to “meet their responsibility to respect children’s rights and to commit to supporting the human rights of children.”<sup>9</sup> Among other things, the Principles state that businesses should “ensure that products and services are safe, and seek to support children’s rights through them.” This includes digital products and services, and would require companies to put suitable protections in place for child users, such as age verification mechanisms, and heightened privacy measures as well as the other aspects of the design Code explored further below.

9. The Committee on the Rights of the Child has published expert guidance on children’s rights and business.<sup>10</sup> In its General Comment no. 16, the Committee asserts that “States should require businesses to undertake child-rights due diligence” in order to “ensure that business enterprises identify, prevent and mitigate their impact on children’s rights including across their business relationships and within global operations.”<sup>11</sup> It is therefore right that the ICO is seeking to develop a Code of practice which is tailored to addressing the rights of children in a context where they face specific risks resulting from the actions of business.

### **Best Interests of the Child**

10. The best interests of the child is one of four General Principles of the Convention on the Rights of the Child, which means that it bears special consideration in the fulfilment of all other rights.<sup>12</sup> It is

---

<sup>7</sup> United Nations Guiding Principles for Business and Human Rights, General Principles.

<sup>8</sup> UNICEF, Save the Children & UN Global Compact, Children’s Rights and Business Principles in Context, 2015 (on file with authors).

<sup>9</sup> Children’s Rights & Business Principles, available at <http://childrenandbusiness.org/>

<sup>10</sup> Committee on the Rights of the Child, General Comment no. 16 on State obligations regarding the impact of the business sector on children’s rights (2013), available at [www2.ohchr.org/english/bodies/crc/docs/gc/crc-c-gc-16\\_en.doc](http://www2.ohchr.org/english/bodies/crc/docs/gc/crc-c-gc-16_en.doc)

<sup>11</sup> CRC General Comment no. 16, para. 62.

<sup>12</sup> See Child Rights International Network, General Principles of the Convention on the Rights of the Child, available at <https://www.crin.org/en/home/rights/themes/general-principles>.

essential that services respect the best interests of children, and this should be done in a clear and consistent manner. Services should be able to explain, through their DPIAs how they have addressed a child's best interests when making decisions about the protections they offer, or use of a child's data for commercial purposes. The Code should require that services explicitly and transparently consider children's best interests and that this assessment takes into consideration variables of age, capacity and other vulnerabilities when determining their course of action.

11. Children's right to be heard, and to have their views taken into consideration, also serves as a General Principle of the Convention on the Rights of the Child.<sup>13</sup> Viewing children's rights **only** through the prism of best interests could fail to recognise the many opportunities children have to exercise their rights online, and ultimately lead to an overly protective approach. The Code should recognise that children's right to be heard and have their views taken into consideration, means they have the right to participate in the digital environment.

### **Children's Rights in a Digital World**

12. In recent years, key resolutions from the United Nations have made clear that children have the same rights online as they do offline.<sup>14</sup> In the digital environment there is often particular attention given to children's rights to protection from violence<sup>15</sup> (including cyberbullying, online grooming, and child sex abuse); privacy<sup>16</sup>; freedom of expression, association, access to information and participation<sup>17</sup>; non-discrimination and education<sup>18</sup>.

13. UNICEF has explored and clarified the public obligation and private responsibility to respect children's rights in a digital world, and in recent years has published global reports, discussion papers

---

<sup>13</sup> See Child Rights International Network, General Principles of the Convention on the Rights of the Child, available at <https://www.crin.org/en/home/rights/themes/general-principles>.

<sup>14</sup> See, e.g., United Nations Human Rights Council Resolution A/HRC/20/L.13 on the promotion, protection and enjoyment of human rights on the Internet, June 2012.

<sup>15</sup> See UNICEF & ITU, Guidelines for Industry on Child Online Protection (2013), available at [www.itu.int/pub/S-GEN-COP.IND-2013](http://www.itu.int/pub/S-GEN-COP.IND-2013).

<sup>16</sup> UNICEF, Discussion Paper Series: Children's Rights and Business in a Digital World, *Privacy, Protection of Personal Information and Reputation* (2017), available at [https://www.unicef.org/csr/css/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_PRIVACY.pdf](https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf).

<sup>17</sup> UNICEF, Discussion Paper Series: Children's Rights and Business in a Digital World, *Freedom of Expression, Association, Access to Information and Participation* (2017), available at [https://www.unicef.org/csr/css/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_EXPRESSION.pdf](https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_EXPRESSION.pdf).

<sup>18</sup> UNICEF, Discussion Paper Series: Children's Rights and Business in a Digital World, *Access to the Internet and Digital Literacy* (2017), available at [https://www.unicef.org/csr/css/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_ACCESS.pdf](https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_ACCESS.pdf).

and practical guidance on the subject.<sup>19</sup> The Committee on the Rights of the Child has noted that “[d]igital media is of particular concern” for children’s rights,<sup>20</sup> and has accepted a proposal from the Children’s Commissioner for England and the London School of Economics to develop a General Comment on Children’s Rights and Digital Media.<sup>21</sup>

14. There is a perceived tension between children’s protection rights and participation rights. For instance, greater protections for children, if taken to the extreme, can risk reducing a child’s participation in the digital world as well as limits their access to other rights such as accessing information about identity and development.<sup>22</sup> Whilst a balance between the principles of child protection and child agency needs to be managed, they are not inherently contradictory. By approaching children’s rights holistically, with a view to advancing all of these rights across the board, it is possible for children to explore and express themselves in the digital world while also enjoying greater privacy protections.

15. A child-rights due diligence approach would require that businesses consider the full range of children’s rights in the digital environment. Among other things, this approach offers a broad foundation for data protection impact assessments and underlies principles for privacy by design. The ICO has likewise already highlighted the need for a risk-based approach in its recent guidance on Children and the EU General Data Protection Regulation (GDPR).<sup>23</sup> The Code should therefore be explicitly grounded in a child-rights due diligence approach, and should aim to foster an inclusive digital world in which all children can fully and safely exercise all of their rights.

## Global Impact

---

<sup>19</sup> See, e.g.; UNICEF, *State of the World’s Children 2017: Children in a Digital World*, available at <https://www.unicef.org/sowc2017/>; UNICEF, *Children’s Online Privacy and Freedom of Expression: Industry Toolkit*, available at [https://www.unicef.org/csr/files/UNICEF\\_Childrens\\_Online\\_Privacy\\_and\\_Freedom\\_of\\_Expression\(1\).pdf](https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf).

<sup>20</sup> CRC General Comment no. 16, para. 60.

<sup>21</sup> Children’s Commissioner for England, *The Case for a UNCRC General Comment on Children’s Rights and Digital Media* (2017), available at <https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Case-for-general-comment-on-digital-media.pdf>.

<sup>22</sup> As above, UNICEF, *Discussion Paper Series: Children’s Rights and Business in a Digital World, Privacy, Protection of Personal Information and Reputation and Freedom of Expression, Association, Access to Information and Participation*

<sup>23</sup> Information Commissioner’s Office, *Children and the GDPR* (2018), available at <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>

16. Given the global nature of business operations and Internet Governance, the Code will undoubtedly impact children's rights outside the United Kingdom. Not only will some companies likely apply the design standards in markets beyond the UK, it is very likely that the Code will be referenced and considered by national, regional and international standard-setting bodies that seek to protect, respect and realise children's rights in a digital world. The Code should remain strongly rooted in international children's rights, and should contemplate probable and possible extraterritorial impacts to ensure it has far-reaching impacts to protect children.

## ASPECTS OF DESIGN

### QUESTION 5A:

17. There is often a tension between what is in children's best interests and what is in a service's best interests, and historically commercial incentives have meant that the service's best interests are given precedence. In the case of ISS providers, responsibility to protect children's privacy has predominantly been outsourced to end users, with either parents or children themselves expected to determine and manage risk, often with incomplete understanding of the implications. The ICO Guidance on Children and the GDPR however makes clear however that the Information Society Services (ISS) provider is responsible for assessing the potential child rights impacts of their practices by means of a data protection impact assessment (DPIA).<sup>24</sup>

18. As explained in further detail below, transparency regarding how best interests have been determined will be essential to ensure that services have adequately considered children's rights and interests, and responsibility is not being pushed down to end users. The principle of transparency is already embedded in the GDPR guidance for children, and key feature of in the Government's consultation response on Internet Safety.<sup>25</sup> The Code should embed transparency as a key principle in protecting and respecting children's rights in the digital environment.

---

<sup>24</sup> As before ICO, Children and the GDPR

<sup>25</sup> HM Government, Government Response to the Internet Safety Strategy Green Paper, (2018) [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/708873/Government\\_Response\\_to\\_the\\_Internet\\_Safety\\_Strategy\\_Green\\_Paper\\_-\\_Final.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf)



## QUESTION 5C

### Default Privacy Settings

19. Children's privacy is better protected when action is required to authorise the sharing or processing of their personal data beyond what is necessary for the service to be delivered. This provides children with higher thresholds of protection by default, and helps children avoid authorising the processing of their personal information without knowledge or consideration – see below for analysis and recommendations on free and meaningful consent. Children are further empowered to protect their privacy when they can easily access and adjust their privacy settings at any time. The Code should ensure that default privacy settings minimise the processing of children's personal data, and should require that privacy settings be easily accessible for children.

20. Default privacy settings are often considered in light of what information children share publicly. For example, social networks provide users with options to limit the reach and flow of the information they share with other users. While it is important that children have control over how others can see their information, privacy settings must also give children control over how services can process and share their information. In this regard, children may have less understanding of the risks involved or be more willing to overlook risks due to their having unclear or less immediate consequences.<sup>26</sup> The Code should consider higher default privacy settings not only in terms of what information children share with other users, but also how services process children's information.

### Data Minimisation Standards

21. Processing children's data may have far-reaching, long-term consequences, from health and education outcomes to employment and access to finance.<sup>27</sup> Given the growing amounts of data generated during childhood, it is especially important that services seek to minimise the data collected from children in order to preserve their future prospects. This is particularly critical where data is being collected for commercial purposes and best interests of the child are unlikely to be served by its collection or use. The Code should establish a strong presumption that children's data should not be collected and processed unless truly necessary.

---

<sup>26</sup> Lareki, Arkaitz & Martínez de Morentin, Juan Ignacio & Altuna, Jon & Amenábar, Nere. (2016). Teenagers' perception of risk behaviors regarding digital technologies. Computers in Human Behavior. 68. 10.1016/j.chb.2016.12.004. Accessed here: <file:///C:/Users/COMeara/Downloads/Articulopublicado2017.pdf>

<sup>27</sup> See, e.g., Wolife Christl, Corporate Surveillance in Everyday Life, Cracked Labs (2017), available at [http://crackedlabs.org/dl/CrackedLabs\\_Christl\\_CorporateSurveillance.pdf](http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf)

## **Presentation and Language of Terms and Conditions and Privacy Notices**

22. A child's privacy is best protected where they provide free and informed consent for the processing of their personal data or, where they lack the capacity to do so, parents or guardians provide this consent on their behalf. Requesting consent for data processing gives children control over how their personal information is used and shared, and empowers children to understand and exercise their right to privacy. The Code should encourage services to seek children's consent as their basis for data processing.

23. Although other legal bases for data processing may exist, obtaining free and informed consent is the approach most consistent with children's rights and best interests. The decision whether to seek consent or rely on other grounds for processing data should not be determined by a user's age. That is, where consent for equivalent data processing would be sought from adults, it must also be sought from or on behalf of children. For example, if a service were to seek consent from adults to share data with third parties, that same service should not share children's data with third parties on the alternative basis of legitimate interests. Notably, one social media company recently adopted this approach and has faced criticism from children's rights advocates for acting outside the spirit of data protection legislation.<sup>28</sup> Such an approach erodes the additional protections to which children are entitled and should not be taken lightly. The Code should discourage requests for consent where data processing is not likely to be in children's best interests, and prohibit the use of other grounds for data processing where consent would be sought from adults.

24. For a child's consent to be valid, it must be sought in a manner and form that matches their level of understanding. Requests for a child's consent must be communicated in plain language and should explore the use of alternative communication methods and innovative techniques, such as icons, diagrams, images and videos, where appropriate to explain how their personal data would be handled. A child's capacity to consent to data processing will necessarily depend on how information is presented to them, and the Code should make clear that a child's consent can only be considered valid when requests are made in a form and manner that they could reasonably be expected to understand.

---

<sup>28</sup> See John Carr, Facebook and the GDPR (2018), available at <https://johnc1912.wordpress.com/2018/04/25/facebook-and-the-gdpr/>

25. For a child's consent to be meaningful, they must also be offered clear, specific and genuine choices about how their data will be processed. These choices should reflect their capacities to understand the choices available and the risks that they face online. Conditioning the use of a service on the provision of personal data runs counter to the voluntary nature of consent and the principle of data minimisation. The Code should discourage all-or-nothing requests for consent and specify which actions require specific, granular consent, for example sharing data with third parties for the purposes of advertising or marketing.

### **Geolocation Technology**

26. Businesses, schools, parents and other individuals may seek to track the precise or approximate location of children. Location data raises particular concerns as it can reveal sensitive data about a child, and potentially put them in danger, as well as more broadly hinder their developing sense of autonomy. Children should be able to clearly see when their location is being tracked, and to understand which service is tracking their location for which purpose. In keeping with views of data minimisation and informed consent, a child's location should not be tracked when they are not actively using a service, and when it is not necessary for the delivery of that service. The Code should restrict the use of geolocation technology, ensure risks to children of gathering location data are considered specifically in DPIAs, and require transparency in tracking children's location.

### **Automated and Semi-Automated Profiling**

27. Advertising and marketing is overwhelmingly data-driven, and children are increasingly targeted with a deluge of tailored commercial messages that seek to direct their behaviour and manipulate emotions in a bid to increase impact of advertising. Profiling children and undermining their privacy for the purpose of monetizing their Internet usage data arguably amounts, under certain circumstances, to economic exploitation.<sup>29</sup> Children may also experience discrimination as a result of digital advertising based on profiling. The spirit and purpose of the GDPR look unfavourably on profiling children for the purposes of advertising or marketing.<sup>30</sup> International industry standards have for years forbidden

---

<sup>29</sup> UNICEF, *Children and Digital Marketing: Rights, risks and opportunities* (2018), pp. 10-11, available at [https://www.unicef.org/csr/files/Children\\_and\\_Digital\\_Marketing\\_-\\_Rights\\_Risks\\_and\\_Opportunities\(2\).pdf](https://www.unicef.org/csr/files/Children_and_Digital_Marketing_-_Rights_Risks_and_Opportunities(2).pdf)

<sup>30</sup> European Union General Data Protection Regulation, Recital 71; Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (2017), available at [ec.europa.eu/newsroom/article29/document.cfm?doc\\_id=49826](http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826)

profiling children below the age of 13 for the purpose of behavioural advertising.<sup>31</sup> It is highly unlikely that profiling children of any age in this manner would be in their best interests, and the Code should prohibit profiling children for the purposes of advertising or marketing.

### **Transparency of Paid-for Activity such as Product Placement and Marketing**

28. It is well-established that young children have not yet developed the ability to distinguish commercial messages from content, and the growing use of data-driven marketing techniques poses challenges for children of all ages.<sup>32</sup> Commercial messages in the digital environment are often less easily identified as such. Behavioural advertising in particular can be both more effective and more difficult to detect, for instance by being embedded into games or learning experiences when children's critical faculties and decision-making processes are compromised.<sup>33</sup> The Code should ensure that any commercial and other paid-for messages targeted to children in the digital environment are clearly identified as such.

### **Sharing and Resale of Data**

29. Sharing and reselling children's personal data can have potential long-term impacts on their future prospects and privacy, with amassed layers of information about them as a person, their preferences and online activities being used to influence their behaviour.<sup>34</sup> Children's data should not be shared with or sold to third parties unless this is in their best interests, and children should not be presented with requests to grant consent for the onward disclosure of their personal data that run manifestly counter to their best interests. It is unlikely that sharing or reselling children's data for the purposes of advertising or marketing would be considered in their best interests. It is noteworthy that the recently passed California Consumer Privacy Act of 2018 requires explicit consent for the sale of the personal information of a child under 16, and allows all consumers to "opt out" out of the onward sale of their

---

<sup>31</sup> Consolidated ICC Code of Advertising and Marketing Communication Practice, s. D.7.4, available at <https://cdn.iccwbo.org/content/uploads/sites/3/2011/08/ICC-Consolidated-Code-of-Advertising-and-Marketing-2011-English.pdf>.

<sup>32</sup> See UNICEF, *A Child Rights-Based Approach to Food Marketing: A Guide for Policy-Makers* (2018) available at [https://www.unicef.org/csr/files/A\\_Child\\_Rights-Based\\_Approach\\_to\\_Food\\_Marketing\\_Report.pdf](https://www.unicef.org/csr/files/A_Child_Rights-Based_Approach_to_Food_Marketing_Report.pdf)

<sup>33</sup> See UNICEF, *Children and Digital Marketing: Rights, risks and opportunities* (2018), available at [https://www.unicef.org/csr/files/Children\\_and\\_Digital\\_Marketing\\_-\\_Rights\\_Risks\\_and\\_Opportunities\(2\).pdf](https://www.unicef.org/csr/files/Children_and_Digital_Marketing_-_Rights_Risks_and_Opportunities(2).pdf)

<sup>34</sup> See UNICEF, Discussion Paper Series: Children's Rights and Business in a Digital World, *Privacy, Protection of Personal Information and Reputation* (2017), available at [https://www.unicef.org/csr/css/UNICEF\\_CRB\\_Digital\\_World\\_Series\\_PRIVACY.pdf](https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf).

data.<sup>35</sup> The Code should prohibit the sharing or reselling of children's personal data unless this can be shown to be in children's best interests and specific, valid consent has been obtained.

### **Strategies used to Encourage Extended User Engagement**

30. The digital world offers children many opportunities to connect, grow and develop, but this should not come at the expense of connecting, growing and developing in the physical world. For instance, limiting their ability to participate in the artistic and cultural life of their community. Technology should facilitate the full exercise of children's rights, and techniques designed to keep children's attention for extended periods of time can run counter to their best interests.<sup>36</sup> The Code should acknowledge persuasive techniques, and should discourage services from deploying strategies to extend user engagement with children.

### **User Reporting and Resolution Processes and Systems**

31. Services set and enforce their own terms, and must be prepared to promptly address potential violations in order for these terms to be effective. Reporting mechanisms should be designed in ways that children can easily access, and children should be advised about their right to initiate complaints. It should be simple and straightforward for children to flag a privacy concern with a service, and children's complaints should be answered and addressed without delay. Decisions should be communicated in a form, manner and language that children can understand, including an explanation of how the decision was reached and what further courses of action are available should the child wish to challenge the decision. The Code should require that reporting mechanisms be made accessible for children, that children's complaints are resolved at speed and within specified timeframes, and that decisions are communicated in an accessible way including information about further courses of action.

32. Familiarity with processes and terminology increases access by children. Whilst services are responsible for designing their own reporting mechanisms, standardization of how mechanisms are accessed and referred to would make it easier for children to apply learning between platforms and services and navigate systems with greater confidence. The Code should establish common elements of process and terminology across user reporting and resolution processes and systems.

---

<sup>35</sup> California Consumer Privacy Act of 2018, available at [https://leginfo.ca.gov/faces/billTextClient.xhtml?bill\\_id=201720180AB375](https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375)

<sup>36</sup> See UNICEF, *Children and Digital Marketing: Rights, risks and opportunities* (2018), available at [https://www.unicef.org/csr/files/Children\\_and\\_Digital\\_Marketing\\_-\\_Rights\\_Risks\\_and\\_Opportunities\(2\).pdf](https://www.unicef.org/csr/files/Children_and_Digital_Marketing_-_Rights_Risks_and_Opportunities(2).pdf)

### **Ability to Understand and Activate a Child's Right to Erasure, Rectification and Restriction**

33. Children merit additional protection for the right to privacy, and should be able to exercise this right through seeking the erasure or correction of their personal data. This right should apply broadly to all data collected during childhood, including data collected with parental consent, and be given additional weight when balancing the child's right to privacy against the right of free of expression held by others. For children and adults whose data were collected during childhood to exercise this right, there must be clear, straightforward and accessible means to seek the deletion or modification of their data.

34. Children should be made aware of their rights to request the correction, modification and deletion of their data when they sign up for a service, and should be reminded of these rights regularly. For example, when a child seeks to remove information from view on a user interface, such as a post or photograph on a social media profile, they should be prompted with an option to request that the service erase and no longer keep a record of this information, rather than simply hide it. The Commission should consider applying time restrictions on consent when given as a child, or on behalf of a child if under the age of digital consent, particularly in relation to data held by services where usage has lapsed for a significant period of time. The Code should recognise a presumption that requests to erase, rectify or restrict data collected during childhood be granted, and should provide guidance as to the suitability and accessibility of processes for making these requests.

### **Ability to Access Advice from Independent, Specialist Advocates on All Data Rights**

35. Children face many barriers to accessing justice when their rights have been infringed, and these can be especially challenging to overcome in the context of business-related abuses and violations.<sup>37</sup> Collective and third-party complaints, such as those brought by child rights advocates or non-governmental organisations, provide a means to raise and remedy abuses and violations of children's rights without needing individual children to come forward. The Code should authorise group and representative complaints to address potential abuses and violations.

### **Privacy by Design**

---

<sup>37</sup> UNICEF and International Commission of Jurists, *Obligations and Actions on Children's Rights and Business: A practical guide for States to implement the (2015)*, available at [https://www.unicef.org/csr/css/CSR\\_GC\\_OBLIGATIONS\\_AND\\_ACTIONS\\_FINAL\\_AUGUST05.pdf](https://www.unicef.org/csr/css/CSR_GC_OBLIGATIONS_AND_ACTIONS_FINAL_AUGUST05.pdf)

36. Data Protection Impact Assessments (DPIAs) are a key component of privacy by design. Building on the corporate responsibility to conduct human rights due diligence, it is essential that DPIAs identify and address potential negative impacts on children's rights in line with the provisions of the UNCRC. The Code should mandate that DPIAs and other means to implement privacy by design principles incorporate specific consideration of children's rights.

37. Transparency is essential to ensure the efficacy of DPIAs. Services should make non-commercially sensitive findings of their DPIAs public to the extent possible, and should be prepared to disclose Assessments to the ICO. Services should be supported to share and cooperate to better across industry and with stakeholders concerned with promoting children's rights to address common industry challenges. The Code should encourage public disclosure of DPIAs, grant authority to review these Assessments, and foster a climate of cooperation among industry peers.

#### **Additional Aspect: Parental Consent**

38. Services will need to seek the consent of parents or legal guardians to process the data of children below the age of 13. There are at present no clear standards on seeking and verifying parental consent, which offers services little guidance and children little protection. The Children's Online Privacy Protection Act (COPPA) in the United States lists means by which services can obtain parental consent and provides for the negotiation of safe harbour agreements, which allow companies to receive certification that they are compliant with COPPA.<sup>38</sup> The Code should establish clear protocols for obtaining valid parental consent.

#### **Additional Aspect: Age Verification**

37. Age verification is an implicit requirement in seeking a child's valid consent for data processing, and the ICO has acknowledged the need for innovation in the development of age verification technology and services.<sup>39</sup> It is feasible for a public or trustworthy third-party service to provide children a means to confirm that they are above the age of consent without sharing their personal data. The Code should encourage the development of technological solutions and seek to establish a universal means by

---

<sup>38</sup> United States Federal Trade Commission, Children's Online Privacy and Protection Rule, available at <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule>.

<sup>39</sup> Information Commissioner's Office, Children and the GDPR (2018), available at <https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf>

which children can validate their consent for data processing without sharing additional personal information.

## **FUTURE CONTRIBUTIONS**

### **QUESTION 6**

Name: [REDACTED]

Email: [REDACTED]

#### **Brief summary of what you think you could offer**

38. UNICEF is glad to contribute to the ICO's work in developing the content of the Code. UNICEF can offer a strong understanding of international children's rights, and how these rights apply in the digital environment on a practical level. UNICEF also enjoys strong links with government, industry, academia and civil society, and could consider convening a multi-stakeholder discussion, consultation or event to further the work of the Commissioner in developing and publicising the Code.

## **FURTHER VIEWS AND EVIDENCE**

### **QUESTION 7**

39. UNICEF commends the efforts of the ICO to develop the Code, and recognises that the Code will require additional resources for adequate enforcement. It is evident that the ICO could benefit from increased budgetary allocations and the development of a dedicated, expert team on children's privacy. The ICO should make clear that additional resources and expertise are required for Code enforcement, and consider ways in which this mandate could be best exercised. It is notable that an eSafety Commissioner has been established in Australia to help children enjoy safe and positive experiences online, and the ICO could consider advocating a similar approach in the United Kingdom.

40. The Code will touch on many policy aspects addressed by other public entities and institutions. For example, the Code will build on the work of the Children's Commissioners across the United Kingdom, and will address aspects of the work of consumer protection and advertising authorities. It will likely interact with areas of Internet governance such as the proposed Social Media Code of Conduct being considered within the upcoming White Paper on Internet Safety. The ICO should seek to coordinate efforts across the Government from an early stage in order to ensure and solidify support for the adoption and enforcement of the Code.



41. Technology is rapidly evolving, and the Code must be seen as a living document. From the outset, the Code should establish an agreed time frame in which it will be reviewed to ensure ongoing effectiveness. Review processes should be transparent and involve consultation with a full range of stake-holders.

## SECTION TWO: ABOUT YOU

Are you:

A body representing the views or interests of children? Please specify: UNICEF works to fully realise all rights of all children in all places.	<input checked="checked" type="checkbox"/>
A body representing the views or interests of parents? Please specify:	<input type="checkbox"/>
A child development expert? Please specify:	<input type="checkbox"/>
A provider of ISS likely to be accessed by children? Please specify:	<input type="checkbox"/>
A trade association representing ISS providers? Please specify:	<input type="checkbox"/>
An ICO employee?	<input type="checkbox"/>
Other? Please specify:	<input type="checkbox"/>